Defeating an Active Adversary Using Difference Families in Groups

Lily Rhodes

August 2026

University of
St Andrews

Supervised by
Dr Sophie Huczynska

1 Introduction and Background Information

1.1 Introduction

First proposed in 2004 by Ogata et al. [11], Algebraic manipulation detection (AMD) codes can be viewed as a game between an encoder and an adversary. An AMD code has the form $(\mathcal{S}, \mathcal{T}, \mathcal{K}, \mathcal{E})$ where $\mathcal{S}$ is a set of sources, $\mathcal{T}$ a set of tags, $\mathcal{K}$ a set of keys and $\mathcal{E}$ a set of encoding functions $E_k : \mathcal{S} \to \mathcal{T}$ corresponding to the keys $k \in \mathcal{K}$. The encoder randomly chooses a secret key and creates pairs (s, t), where $s \in \mathcal{S}$ and $t \in \mathcal{T}$, of sources and tags using the corresponding E_k. An adversary, knowing a pair (s, t), then aims to create a fake pair (s', t') that could be accepted as a real pair.

We present a simple example (a more generalised version of this is given in [12](Example 1.1)):

Example 1.1. Let $\mathcal{S} = \mathcal{T} = \{0, 1\}$. Define $\mathcal{K} = \{0, 1\} \times \{0, 1\}$. For every $(a, b) \in \mathcal{K}$ define the encoding function $E_k : \mathcal{S} \to \mathcal{T}$ such that $s \mapsto as + b$ for all $s \in \mathcal{S}$. Hence we have $E_{(0,0)} = 0, E_{(0,1)} = 1, E_{(1,0)} = s$ and $E_{(1,1)} = s + 1$. In this set up, if we were to choose a pair (s, t), say $(0, 1)$, then this would be valid with $k = (0, 1)$ or $k = (1, 1)$. Hence, if the adversary were to present this pair, they have a success probability of $\frac{2}{4} = \frac{1}{2}$.

Paterson and Stinson propose many constructions for AMD codes using different types of difference structures in finite abelian groups [12]. In this paper we focus on Generalised Strong External Difference Families (GSEDFs). In order to define this we introduce the following notation:

Let G be an additive group with $A_1, A_2 \subseteq G$. Then $\Delta(A_1, A_2)$ is the multiset $\{x - y : x \in A_1, y \in A_2\}$ and, for $A \subseteq G, \Delta(A)$ is the multiset $\{x - y : x \in A, y \in A, x \neq y\}$. Alternatively, in a multiplicative group $\Delta(A_1, A_2)$ is the multiset $\{xy^{-1} : x \in A_1, y \in A_2\}$ and, $\Delta(A)$ is the multiset $\{xy^{-1} : x \in A, y \in A, x \neq y\}$. Here, a multiset is a set that may have repeated entries. If an element x appears n times in a multiset, we say x has multiplicity n.

Definition 1.2 (Difference Set)**.** Let G be an abelian group of order v. A (v, k, λ) difference set is a subset A of G such that the following multiset equation holds:

$$\Delta(A) = \lambda(G \backslash \{0\}) \tag{1}$$

From difference sets we can construct various combinatorial structures known as difference families.

Definition 1.3 (Difference Family)**.** Let G be an abelian group of order v. Let $A_1, A_2, ..., A_m$ be mutually disjoint subsets of G each of size k. Then $\{A_1, A_2, ..., A_m\}$ is a (v, m, k, λ)- difference family ((v, m, k, λ)-DF) if the following multiset equation holds:

$$\bigcup_{1 \leq i \leq m} \Delta(A_i) = \lambda(G \backslash \{0\}) \tag{2}$$

Definition 1.4 (External Difference Family)**.** Let G be an abelian group of order v. Let $A_1, A_2, ..., A_m$ be mutually disjoint subsets of G each of size k. Then $\{A_1, A_2, ..., A_m\}$ is a (v, m, k, λ)-external difference family ((v, m, k, λ)-EDF) if the following multiset equation holds:

$$\bigcup_{1 \leq i \leq m} \Big(\bigcup_{1 \leq j \leq m, j \neq i} \Delta(A_i, A_j) \Big) = \lambda(G \backslash \{0\}) \tag{3}$$

Definition 1.5 (Strong External Difference Family)**.** Let G be an abelian group of order v. Let $A_1, A_2, ..., A_m$ be mutually disjoint subsets of G each of size k. Then $\{A_1, A_2, ..., A_m\}$ is a (v, m, k, λ)-strong external difference family ((v, m, k, λ)-SEDF) if the following multiset equation holds for all $1 \leq i \leq m$:

$$\bigcup_{1 \leq j \leq m, j \neq i} \Delta(A_i, A_j) = \lambda(G \backslash \{0\}) \tag{4}$$

We can then consider a more generalised version of SEDFs by allowing the subsets to have different sizes.

Definition 1.6 (Generalised Strong External Difference Family)**.** Let G be an abelian group of order v. Let $A_1, A_2, ..., A_m$ be mutually disjoint subsets of G with $|A_i| = k_i$ for all $1 \leq i \leq m$. Then $\{A_1, A_2, ..., A_m\}$ is a $(v, m; k_1, k_2, \ldots, k_m; \lambda_1, \lambda_2, \ldots, \lambda_m)$-generalised strong external difference family ($(v, m; k_1, k_2, \ldots, k_m; \lambda_1, \lambda_2, \ldots, \lambda_m)$-GSEDF) if the following multiset equation holds for all $1 \leq i \leq m$:

$$\bigcup_{1 \leq j \leq m, j \neq i} \Delta(A_i, A_j) = \lambda_i(G \backslash \{0\}) \tag{5}$$

Hence a (v, m, k, λ)-SEDF is a $(v, m; k, \ldots, k; \lambda, \ldots, \lambda)$-GSEDF.

By comparing data from a computer search, and known constructions from literature, this paper aims to comprehensively analyse constructions of GSEDFs and propose potentially new methods of construction.

1.2 A Brief Background in Group Theory

Every GSEDF exists within a mathematical structure known as a group. Here, we briefly define the fundamental concepts of group theory that underpin the further results. For a more detailed introduction to group theory see [1].

Definition 1.7 (Binary Operation)**.** A Binary Operation is a function $* : X \times X \to X$, where X is a non empty set.

Definition 1.8 (Group)**.** A group is a non empty set G, with a binary operation $*$, such that the following properties are satisfied:

(i) Associativity: $(x * y) * z = x * (y * z), \forall x, y, z \in G$.

(ii) Identity Element: $\exists 1 \in G$ s.t. $x * 1 = 1 * x = x, \forall x \in G$.

(iii) Inverses: $\forall x \in G, \exists x^{-1} \in G$ s.t. $x * x^{-1} = x^{-1} * x = 1$.

Example 1.9. The integers $\mathbb{Z}$, with addition form a group.

Proof. Binary Operation: If $x, y \in \mathbb{Z}$ then $x + y \in \mathbb{Z}$.
Associativity: Let $x, y, z \in \mathbb{Z}$ then $(x + y) + z = x + y + z = x + (y + z)$.
Identity Element: $0 \in \mathbb{Z}$ and for $x \in \mathbb{Z}, x + 0 = 0 + x = x$.
Inverses: If $x \in \mathbb{Z}$ then $-x \in \mathbb{Z}$ and $x + -x = -x + x = 0$. □

Definition 1.10 (Abelian Group)**.** A group G is abelian if the binary operation $*$ is commutative. That is, $\forall x, y \in G, x * y = y * x$.

Example 1.11. The example in 1.9 is an abelian group as $x + y = y + x, \forall x, y \in \mathbb{Z}$.

Definition 1.12 (Subgroup)**.** A subgroup is a subset H of a group G that is itself a group with the same operation as G. We write $H \leq G$.

Definition 1.13 (Cosets)**.** Let G be a group and $H \leq G$. Then, for a fixed element $g \in G$, the right coset is defined as

$$Hg = \{hg : h \in H\}$$

and the left coset is defined as

$$gH = \{gh : h \in H\}$$

In an abelian group $gh = hg$ for all $g, h \in G$. Hence, since $H \leq G$, $gH = Hg$ and so we can refer to these simply as cosets.

Definition 1.14 (Order of an Element)**.** An element x of a group G has order $n \in \mathbb{Z}$ if n is the smallest positive integer such that $x^n = 1$.

The order of an element in a group G must divide the order of G. The proof of this statement is given in [1](Theorem 1.5.16).

Definition 1.15 (Generator)**.** Let S be a nonempty subset of a group G. $\langle S \rangle$ is the group generated by S which is the intersection of all subgroups of G containing S. Hence $\langle S \rangle$ is the smallest subgroup that contains S.

Definition 1.16 (Cyclic Group)**.** We say a G group is cyclic if it is generated by a single element and can write $G = \langle g \rangle$.

Given two cyclic groups we can create a third, not necessarily cyclic, group using direct products.

Definition 1.17 (Direct Product)**.** Let G and H be groups with operations $*_G$ and $*_H$ respectively. Then the direct product is a set $G \times H = \{(g, h); g \in G, h \in H\}$ with the component wise operation $*$ such that

$$(g_1, h_1) * (g_2, h_2) = (g_1 *_G g_2, h_1 *_H h_2)$$

.

These groups can be represented in many different ways. To simplify the classification of groups we define a notion of equivalence between two groups.

Definition 1.18 (Isomorphism)**.** Let G, H be groups. We say G and H are isomorphic, and write $G \cong H$, if there exists a bijection $\phi : G \to H$ such that $\phi(gh) = \phi(g)\phi(h)$.

If $\phi : G \to H$ is not a bijection but still satisfies $\phi(gh) = \phi(g)\phi(h)$, then ϕ is a homomorphism

Theorem 1.19. The direct product between two cyclic groups C_n, C_m, that have order n and m respectively, is isomorphic to the cyclic group C_{nm}, of order nm, if and only if n and m are coprime. That is, $gcd(n, m) = 1$.

Proof. Omitted, see [1](Proposition 2.5.16). □

Definition 1.20. (Automorphism) An automorphism is an isomorphism from a group G to itself. We call the group of all automorphisms of G $Aut(G)$.

We can consider a generalisation of direct products known as semidirect products.

Definition 1.21 (Semidirect Product)**.** Let G, H be groups with operations $*_G$ and $*_H$ respectively. Let $\phi : H \to Aut(H)$ be an homomorphism. Then the corresponding semidirect product $G \rtimes_\phi H$ is the set $G \times H = \{(g, h) : g \in G, h \in H\}$ with the operation $*$ defined by $(g_1, h_2) * (g_2, h_2) = (g_1 *_G \phi_{h_1}(g_2), h_1 *_H h_2)$.

By introducing a secondary binary operation, we can add additional structure to a group

Definition 1.22 (Ring)**.** A ring is a non empty set G, with two binary operations $*_1$ and $*_2$, such that the following properties are satisfied:

(i) Associativity: $(x *_1 y) *_1 z = x *_1 (y *_1 z), \forall x, y, z \in G$. Additionally, $(x *_2 y) *_2 z = x *_2 (y *_2 z), \forall x, y, z \in G$.

(ii) Identity Element: $\exists 1 \in G$ s.t. $x *_1 1 = 1 *_1 x = x, \forall x \in G$.

(iii) Inverses: $\forall x \in G, \exists x^{-1} \in G$ s.t. $x *_1 x^{-1} = x^{-1} *_1 x = 1$.

Hence, a ring consists of a group with binary operation, combined with a second associative binary operation. Throughout this paper, and in general, these operations are referred to as addition and multiplication.

Example 1.23. The integers $\mathbb{Z}$, form a ring under addition and multiplication.

Proof. From example 1.9, we known that $\mathbb{Z}$ is a group under addition so we need only check multiplication is associative.
For all $x, y, z \in \mathbb{Z}$

$$(xy)z = xyz = x(yz)$$

□

Definition 1.24 (Field)**.** A field is a non empty set G, with two binary operations $*_1$ and $*_2$, such that the following properties are satisfied:
First operation:

(i) Associativity: $(x *_1 y) *_1 z = x *_1 (y *_1 z), \forall x, y, z \in G$.

(ii) Identity Element: $\exists 1 \in G$ s.t. $x *_1 1 = 1 *_1 x = x, \forall x \in G$.

(iii) Inverses: $\forall x \in G, \exists x^{-1} \in G$ s.t. $x *_1 x^{-1} = x^{-1} *_1 x = 1$.

Second operation:

(i) Associativity: $(x *_2 y) *_2 z = x *_2 (y *_2 z), \forall x, y, z \in G\backslash\{0\}$.

(ii) Identity Element: $\exists 1 \in G$ s.t. $x *_2 1 = 1 *_2 x = x, \forall x \in G\backslash\{0\}$.

(iii) Inverses: $\forall x \in G\backslash\{0\}, \exists x^{-1} \in G\backslash\{0\}$ s.t. $x *_2 x^{-1} = x^{-1} *_2 x = 1$.

Example 1.25. The integers $\mathbb{Z}$ do not form a field under addition and multiplication as not every element has a multiplicative inverse.
For example, $3(\frac{1}{3}) = (\frac{1}{3})3 = 1$ but $\frac{1}{3} \notin \mathbb{Z}$. However, rationals $\mathbb{Q}$ do form a field with these operations.

1.3 Some General Results About GSEDFs

Lemma 1.26. [10] If there exists a $(v, m; k_1, \ldots, k_m; \lambda_1, \ldots, \lambda_m)$-GSEDF in a group G of size v then for all $1 \leq i \leq m$,

$$\lambda_i(v-1) = \sum_{j=1, i\neq j}^{m} k_i k_j \tag{6}$$

Proof. This follows from (5) in Definition 1.6. □

Theorem 1.27. [10](Theorem 4.3) If there exists a $(v, 2; k_1, k_2; \lambda_1, \lambda_2)$-GSEDF, then $\lambda_1 = \lambda_2$. Furthermore, if k_1 and k_2 are prime then $\lambda_1 = \lambda_2 = 1$

Proof. (6) tells us that $\lambda_1(v-1) = k_1k_2$, and $\lambda_2(v-1) = k_1k_2$, so $\lambda_1(v-1) = \lambda_2(v-1) \implies \lambda_1 = \lambda_2$. Also, $\lambda_1 | k_1k_2$, and $\lambda_1 < k_1, k_2$. Since k_1, k_2 are prime, we get $\lambda_1 = 1$ and hence $\lambda_2 = 1$. □

Example 1.28. $\{\{0, 1\}, \{2, 4\}\}$ is a $(5, 2; 2, 2; 1, 1)$-GSEDF in $\mathbb{Z}_5$. The subtraction table for this is,

	0	1
2	3	4
4	1	2

Adding 1 to both of these sets gives,

$$\{\{1,2\},\{3,0\}\}$$

which is also a $(5,2;2,2;1,1)$-GSEDF in $\mathbb{Z}_5$, with the same subtraction table as the GSEDF above.

	1	2
3	3	4
0	1	2

Hence these are two equivalent GSEDFs. In fact, we can add any element $n \in \mathbb{Z}_5$ and have a GSEDF equivalent to the first one.

More formally:

$$\begin{aligned}\Delta(A_i+g, A_j+g) &= \{(x+g)-(y+g) : x \in A_i, y \in A_j\} \\ &= \{x-y : x \in A_i, y \in A_j\} \\ &= \Delta(A_i, A_j)\end{aligned}$$

Hence, given a GSEDF we can produce several equivalent GSEDFs by adding a constant. If $\{A_1,\ldots,A_m\}$ is a $(v,m;k_1,\ldots,k_m;\lambda_1,\ldots,\lambda_m)$-GSEDF in G, then for all $g \in G$, $\{A_1+g,\ldots,A_m+g\}$ is an equivalent $(v,m;k_1,\ldots,k_m;\lambda_1,\ldots,\lambda_m)$-GSEDF in G.

2 Constructions Using Near Factorisations

Definition 2.1. (Near Factorisation) Let G be a finite additive group with identity e. A near factorisation of G is a pair of subsets (S,T) such that $G\backslash\{e\} = ST$. That is, for every $g \in G\backslash\{e\}$, g can be written uniquely as $g = st$ for some $s \in S, t \in T$. In an additive group, this becomes $G\backslash\{0\} = S+T$. We call (S,T) an (s,t) near factorisation where $s = |S|$ and $t = |T|$.

First proposed by Caen et al. in 1990 [3], near factorisations can be used to construct GSEDFs. For simplicity we work in the additive group here, but the result follows analogously in the multiplicative group. Given a near factorisation (S,T) of a group G, $G\backslash\{0\} = S+T = S-(-T)$, which is equal to the multiset $\{s-(-t); s \in S, t \in T\} = \Delta(S,-T)$. Hence, $\{S,-T\}$ is a $(v,2;s,t;1,1)$-GSEDF where $v = |G|, s = |S|$ and $t = |T|$.

Lemma 2.2. [8](Lemma 1.1) Let G be a finite group. There exists an (s,t) near factorisation of G if and only if there exists a (t,s) near factorisation of G.

Proof. Suppose (S,T) is a (s,t) near factorisation. Then $|S| = s, |T| = t$ and $ST = G\backslash\{0\}$. $ST = G\backslash\{0\}$ if and only if $(ST)^{-1} = G\backslash\{0\}$. $(ST)^{-1} = T^{-1}S^{-1} = G\backslash\{0\}$. So (S,T) is an (s,t) near factorisation of G if and only if (T^{-1}, S^{-1}) is a (t,s) near factorisation of G. □

In [7], Kreher et al. extend the definition of a near factorisation allowing for cases where $\lambda(G\backslash\{0\}) = S + T$.

Definition 2.3. Let G be a finite additive group with identity e. A λ-fold near factorisation of G is a pair of subsets (S,T) such that $\lambda(G\backslash\{e\}) = ST$. In an additive group this becomes $\lambda(G\backslash\{0\}) = S + T$.

In an abelian group of order v, $ST = G\backslash\{0\} \implies TS = G\backslash\{0\}$ and so (T,S) is a (t,s) near factorisation. In particular, as shown above $\{T, -S\}$ is a $(v, 2; t, s; 1, 1)$-GSEDF in G.

In [9], Kreher et al. show the converse of this argument which allows us to classify all GSEDFs of this form with the following statement.

Lemma 2.4. [9](Lemma 1.6) Let G be an additive group of order v. Then there exists an (s,t) near factorisation of G if and only if there exists a $(v, 2; s, t; 1, 1)$-GSEDF.

Proof. Suppose (S,T) is a (s,t) near factorisation of G. Then we have already shown $(S, -T)$ is a $(v, 2; s, t; 1, 1)$- GSEDF in G. Conversely, if $\{A_1, A_2\}$ is a $(v, 2; s, t; 1, 1)$-GSEDF in G, then $G\backslash\{0\} = \Delta(A_1, A_2) = \{x - y : x \in A_1, y \in A_2\} = A_1 - A_2$. Hence, $(A_1, -A_2)$ is an (s,t) near factorisation in G. □

Observe that $ST = G\backslash\{0\} \implies |S||T| = |G| - 1$. Hence, Lemma 2.4 provides the construction behind the following theorem.

Theorem 2.5. [10](Theorem 4.2) There exists a $(v, m; k_1, \ldots, k_m; 1, \ldots 1)$-GSEDF if and only if, $m = 2$ and $v = k_1k_2 + 1$, or $k_i = 1$ for $1 \leq i \leq m$ and $v = m$.

Proof. We first verify $m = 2$. Suppose (for contradiction) that $\{A_1, \ldots, A_m\}$ is a $(v, m; k_1, \ldots, k_m; 1, \ldots, 1)$-GSEDF in G, where $m \geq 3$ and $k_i > 1$ for

some $1 \leq i \leq m$. Without loss of generality, we can assume $k_1 > 1$. Since we have a GSEDF with $\lambda_i = 1$ for all $1 \leq i \leq m$, (5) gives us

$$\bigcup_{1 \leq j \leq m, j \neq i} \Delta(A_i, A_j) = G \backslash \{0\}$$

and so,

$$\bigcup_{1 \leq i \leq m} \Big(\bigcup_{1 \leq j \leq m, j \neq i} \Delta(A_i, A_j) \Big) = m \cdot (G \backslash \{0\})$$

Hence, we have

$$\bigcup_{2 \leq i \leq m} \Big(\bigcup_{1 \leq j \leq m, j \neq i} \Delta(A_i, A_j) \Big) = (m-2)(G \backslash \{0\}) \tag{7}$$

Since $|A_1| > 1$, let $x, y \in A_1$ and $x \neq y$. Then $A_1 \subset G \implies x, y \in G$ so $x - y \in G$. Hence, as $m \geq 3$ and from (2), there exist $u \in A_i$ and $v \in D_j$, where $i, j > 1$ and $i \neq j$ such that $u - v = x - y$. $u - v = x - y \implies u - x = v - y$. Therefore, $\mu = u - x = v - y$ will appear twice in

$$\bigcup_{1 \leq j \leq m, j \neq i} \Delta(A_i, A_j)$$

which contradicts $\lambda_1 = 1$.

Hence, we need only to consider $m = 2$ or $k_i = 1$ for all $1 \leq i \leq m$. When $m = 2$, from Theorem 1.27 we have $1(v-1) = k_1 k_2$, which gives $v = k_1 k_2 + 1$ as required. Similarly, when $k_i = 1$ we get $1(v-1) = (m-1)1^2$ so $v = m$. $\square$

This gives us the condition for the existence of $(v, 2; k_1, k_2; 1, 1)$-GSEDFs, and Lemma 2.4 shows that all GSEDFs of this form arise from near factorisations. We now discuss a more explicit way to construct examples of these GSEDFs.

Example 2.6. In the cyclic group $\mathbb{Z}_{16}$ of order 16, we have a $(16, 2; 3, 5; 1, 1)$-GSEDF given by the blocks $A_1 = \{1, 2, 3\}, A_2 = \{0, 4, 7, 10, 13\}$. To see this GSEDF as a near factorisation, we take the negative of A_2 (although the same can be done using A_1 as we are in an abelian group). Looking at the addition table we can observe a pattern:

	1	2	3
0	1	2	3
3	4	5	6
6	7	8	9
9	10	11	12
12	13	14	15

Each element of $\mathbb{Z}_{16}$ is present exactly once: beginning with 1 in the top left, and adding 1 across a row and 3 down a column. Indeed, we can see the same arithmetic progression in A_1 and $-A_2$ themselves, with $-A_2$ being the multiples of three from $3 \cdot 0$ to $3 \cdot 4$.

We are able to generalise this example into a concrete construction within cyclic groups.

Theorem 2.7. [3](Example 1) Let $\mathbb{Z}_n$ be the cyclic group of order n, and let s and t be integers such that $n - 1 = st$. Then

$$\{\{1, 2, \ldots, s\}, \{0, s, 2s, \ldots, (t-1)s\}\}$$

is a near factorisation of $\mathbb{Z}_n$.

Proof. Consider the addition table:

	1	2	...	s
0	1	2	...	s
s	$1+s$	$2+s$	...	$2s$
$2s$	$2s+1$	$2s+2$	...	$3s$
$\vdots$	$\vdots$			$\vdots$
$(t-1)s$	$(t-1)s+1$	$(t-1)s+2$	...	ts

This presents the same pattern as in Example 2.6. The first row has every element from 1 to s, the second row from $s+1$ to $2s$, and so on, reaching the highest value of $ts = n - 1$. Since $n - 1 < n$, no value repeats, and so every element of $\mathbb{Z}_n$ appears exactly once. Hence, $\{1, 2, \ldots, s\}\{0, s, 2s, \ldots, (t-1)s\} = \mathbb{Z}_n \backslash \{0\}$. □

This construction produces a valid near factorisation, and hence GSEDF, for all $n \in \mathbb{N}, n > 1$. However, when $n - 1$ is prime, s or t must be one, and so the example is trivial. In [3], Caen et al. extend this near factorisation by

further factorising t, but this does not yield new, non-equivalent GSEDFs as the further construction fails the disjoint condition.

We now have an explanation for the $(v, 2; k_1, k_2; 1, 1)$-GSEDFs in all cyclic groups of order $v = k_1k_2+1$, however, within the data we frequently observed a similar construction within the dihedral group of the same order.

Definition 2.8. The dihedral group D_{2n} of order $2n$, is the semidirect product $\mathbb{Z}_n \rtimes \mathbb{Z}_2$, defined by the homomorphism $\phi : \mathbb{Z}_2 \to Aut(\mathbb{Z}_n)$ where,

$$\phi_x(y) = \begin{cases} y & x = 0 \\ -y & x = 1 \end{cases}$$

When n is odd, Theorem 1.19 tells us that $\mathbb{Z}_{2n} \cong \mathbb{Z}_n \times \mathbb{Z}_2$, and so converting the near factorisation from the cyclic to dihedral group appears to be equivalent to converting from the direct product with $\mathbb{Z}_2$ to the semidirect product with $\mathbb{Z}_2$. The following theorem is an extension of [13](Lemma 6) modified to allow for multisets and hence λ-fold near factorisations not just near factorisations.

Theorem 2.9. Let G be an abelian group. Let X and Y be multisubsets of the multiset $\lambda(G \times \mathbb{Z}_2)$ for some $\lambda \in \mathbb{N}$, with the usual operation $*$, such that $X = -X$ and $Y = -Y$. Then X and Y are also multisubsets of $\lambda(G \rtimes_\phi \mathbb{Z}_2)$, where the operation $*_\phi$ is the that of the dihedral group. Furthermore, $X *_\phi Y = X * Y$.

To prove Theorem 2.9, we will use the following fact about multiplicities of elements in multisets.

Lemma 2.10. Let X and Y be multisets, and let x be an element of X with multiplicity $\mu_X(x)$. Similarly, let y be an element of Y with multiplicity $\mu_Y(y)$. Then the multiplicity of (x, y) in the semidirect product $X \rtimes_\phi Y$ defined by the homomorphism ϕ is,

$$\mu_{X \rtimes_\phi Y}((x, y)) = \mu_X(x) \cdot \mu_Y(y)$$

Proof. We recall from Definition 1.21 that the underlying set of a semidirect product $X \rtimes_\phi Y$, is the cartestian product $X \times Y$. This is well defined in multiset theory by Blizard [2]. Hence, if x appears $\mu_X(x)$ times in X, and y appears $\mu_Y(y)$ times in Y, (x, y) must appear $\mu_X(x) \cdot \mu_Y(y)$ times in $X \times Y$ by the definition of the cartesian product with multisets. □

Proof of Theorem 2.9. We denote by $*_G$ the operation in G, $*_2$ the operation in $\mathbb{Z}_2$, $*$ the operation in $G \times \mathbb{Z}_2$, and $*_\phi$ the operation in $G \rtimes \mathbb{Z}_2$.

Let (x_1, x_2) be an element of X with multiplicity $\mu_X((x_1, x_2))$, and similarly let (y_1, y_2) be an element of Y with multiplicity $\mu_Y((y_1, y_2))$. Then $(x_1, x_2) *_\phi (y_1, y_2) \in X *_\phi Y$.

We first show $X *_\phi Y \subseteq X * Y$, and
$\mu_{X*_\phi Y}((x_1, x_2) *_\phi (y_1, y_2)) \leq \mu_{X*Y}((x_1, x_2) * (y_1, y_2))$.

If $x_2 = 0$:

$$\begin{aligned}(x_1, x_2) *_\phi (y_1, y_2) &= (x_1 *_G \phi_0(y_1), x_2 *_2 y_2) \\ &= (x_1 *_G y_1, x_2 *_2 y_2) \\ &= (x_1, x_2) * (y_1, y_2) \in X * Y\end{aligned}$$

If $x_2 = 1$:

$$\begin{aligned}(x_1, x_2) *_\phi (y_1, y_2) &= (x_1 *_G \phi_1(y_1), x_2 *_2 y_2) \\ &= (x_1 *_G -y_1, x_2 *_2 y_2) \\ &= (x_1 *_G -y_1, x_2 *_2 -y_2) \text{ as } y_2 \in \mathbb{Z}_2 \text{ so } y_2 = -y_2 \\ &= (x_1, x_2) * (-y_1, -y_2) \in X * Y \\ &\text{as } Y = -Y \text{ so } (-y_1, -y_2) \in Y\end{aligned}$$

So $(x_1, x_2) *_\phi (y_1, y_2) \in X * Y$, so $X *_\phi Y \subseteq X * Y$.

For the latter statement, $\mu_X(x) \leq \mu_X(x)$ and $\mu_Y(y) \leq \mu_Y(y)$ hence, since multiplicities are positive integers:

$$\begin{aligned}\mu_{X*_\phi Y}((x_1, x_2) *_\phi (y_1, y_2)) &= \mu_X((x_1, x_2)) \cdot \mu_Y((y_1, y_2)) \text{ by Lemma 2.10} \\ &\leq \mu_X((x_1, x_2)) \cdot \mu_Y((y_1, y_2)) \text{ from above} \\ &= \mu_{X*Y}((x_1, x_2) * (y_1, y_2)) \text{ by Lemma 2.10}\end{aligned}$$

So $\mu_{X*_\phi Y}((x_1, x_2) *_\phi (y_1, y_2)) \leq \mu_{X*Y}((x_1, x_2) * (y_1, y_2))$.
Conversely, for all $(x_1, x_2) * (y_1, y_2) \in X * Y$

If $x_2 = 0$:

$$\begin{aligned}(x_1, x_2) * (y_1, y_2) &= (x_1 *_G y_1, x_2 *_2 y_2) \\ &= (x_1 *_G \phi(y_1), x_2 *_2 y_2) \\ &= (x_1, x_2) *_\phi (y_1, y_2) \in X *_\phi Y\end{aligned}$$

If $x_2 = 1$:

$$\begin{aligned}(x_1, x_2) *_(y_1, y_2) &= (x_1 *_G y_1, x_2 *_2 y_2) \\ &= (x_1 *_G -(-y_1), x_2 *_2 -y_2) \text{ as } y_2 \in \mathbb{Z}_2 \text{ so } y_2 = -y_2 \\ &= (x_1 *_G \phi(-y_1), x_2 *_2 -y_2) \\ &= (x_1, x_2) *_\phi (-y_1, -y_2) \in X *_\phi Y \\ &\text{as } Y = -Y \text{ so } (-y_1, -y_2) \in Y\end{aligned}$$

Hence, $(x_1, x_2) * (y_1, y_2) \in X *_\Gamma Y$ for all $(x_1, x_2) \in X, (y_1, y_2) \in Y$

Again, for the latter statement, $\mu_X(x) \leq \mu_X(x)$ and $\mu_Y(y) \leq \mu_Y(y)$ hence, since multiplicities are positive integers:

$$\begin{aligned}\mu_{X*Y}((x_1, x_2) * (y_1, y_2)) &= \mu_X((x_1, x_2)) \cdot \mu_Y((y_1, y_2)) \text{ by Lemma 2.10} \\ &\leq \mu_X((x_1, x_2)) \cdot \mu_Y((y_1, y_2)) \text{ from above} \\ &= \mu_{X*_\phi Y}((x_1, x_2)_\phi * (y_1, y_2)) \text{ by Lemma 2.10}\end{aligned}$$

So $\mu_{X*_\phi Y}((x_1, x_2) *_\phi (y_1, y_2)) = \mu_{X*Y}((x_1, x_2) * (y_1, y_2))$, and so $X *_\Gamma Y = X * Y$. □

Remark. Here we only require G to be abelian not specifically cyclic as the same transformation can be done coming from an abelian direct product.

Therefore, if our near factorisation (S, T), of $\mathbb{Z}_{2n}$ for odd n, satisfies the property that $S = -S$ and $T = -T$, then $ST = \mathbb{Z}_{2n} \backslash \{0\} = (\mathbb{Z}_n \times \mathbb{Z}_2) \backslash \{0\}$ in the direct product, implies $ST = (\mathbb{Z}_n \rtimes \mathbb{Z}_2) \backslash \{0\}$ in the semidirect product, and so (S, T) is a near factorisation of D_{2n} also.

Example 2.11. $\{\{1, 2, 3\}, \{0, 3, 6\}\}$ is a $(10, 2; 3, 3; 1, 1)$-SEDF in $\mathbb{Z}_{10}$. Writing this equivalently in $\mathbb{Z}_5 \times \mathbb{Z}_2$ gives,

$$\{\{(1, 1), (2, 0), (3, 1)\}, \{(0, 0), (3, 1), (1, 0)\}$$

Recall from Example 1.28, we can add a constant and retain an equivalent SEDF. In the context of near factorisations, this means adding a constant to one set and subtracting the same constant from the other. Adding/subtracting $(3, 0)$ gives,

$$S = \{(4, 1), (0, 0), (1, 1)\}, T = \{(2, 0), (0, 1), (3, 0)\}$$

and now we have (S, T) such that,

$$-S = \{(1, 1), (0, 0), 4, 1)\} = S$$

and

$$-T = \{(3,0),(0,1),(2,0)\} = T$$

which satisfy our conditions in Theorem 2.9.

Hence, (S,T) is a near factorisation of $\mathbb{Z}_5 \rtimes \mathbb{Z}_2 = D_{10}$. To verify this, we check the addition table using dihedral operations.

	$(0,0)$	$(1,1)$	$(4,1)$
$(0,1)$	$(0,1)$	$(1,0)$	$(4,0)$
$(2,0)$	$(2,0)$	$(4,1)$	$(2,1)$
$(3,0)$	$(3,0)$	$(3,1)$	$(1,1)$

And so we have converted a near factorisation, and hence GSEDF, from the cyclic group of order $2n$ to the dihedral group of order $2n$.

The ability to convert the cyclic group of order $2n$ to $\mathbb{Z}_n \times \mathbb{Z}_2$ relies on n being odd. However, in $\mathbb{Z}_{16}$ there is a $(16,2;3,5;1,1)$-GSEDF in both $\mathbb{Z}_{16}$ and D_{16}, yet $n = 8$ is even.

Theorem 2.12. [3](Example 2) For any factorisation $2n-1 = \alpha k$, we have a near factorisation (S,T) of D_{2n} where

$$S = \{(i,0) : 1 \le i \le \frac{k-1}{2}\} \cup \{(i,1) : 0 \le i \le \frac{k-1}{2}\}$$

and

$$T = \{(jk,0) : 0 \le j \le \frac{\alpha-1}{2}\} \cup \{(jk,1) : 0 < j \le \frac{\alpha-1}{2}\}$$

Proof. First, note that when $j = \frac{\alpha-1}{2}$,

$$jk = \frac{\alpha-1}{2}k = \frac{\alpha k - k}{2} = \frac{2n-1-k}{2} = n - \frac{k+1}{2} \equiv -\frac{k+1}{2} \text{mod n}$$

Also,

$$\frac{k-1}{2} + jk = \frac{k-1}{2} - \frac{k+1}{2} = \frac{-2}{2} = -1 = n-1$$

Consider the addition table of S and T in D_{2n}:

	$(1,0)$	$(2,0)$	$\dots$	$(\frac{k-1}{2},0)$	$(0,1)$	$(1,1)$	$\dots$	$(\frac{k-1}{2},1)$
$(0,0)$	$(1,0)$	$(2,0)$	$\dots$	$(\frac{k-1}{2},0)$	$(0,1)$	$(1,1)$	$\dots$	$(\frac{k-1}{2},1)$
$(k,0)$	$(1+k,0)$	$(2+k,0)$	$\dots$	$(\frac{3k-1}{2},0)$	$(-k,1)$	$(1-k,1)$	$\dots$	$(\frac{k-1}{2}-k,1)$
$\vdots$	$\vdots$			$\vdots$	$\vdots$			$\vdots$
$(-\frac{k+1}{2},0)$	$(1-\frac{k+1}{2},0)$	$(2-\frac{k+1}{2},0)$	$\dots$	$(n-1,0)$	$(\frac{k+1}{2},1)$	$(1+\frac{k+1}{2},1)$	$\dots$	$(k,1)$
$(-\frac{k+1}{2},1)$	$(1-\frac{k+1}{2},1)$	$(2-\frac{k+1}{2},1)$	$\dots$	$(n-1,1)$	$(\frac{k+1}{2},0)$	$(1+\frac{k+1}{2},0)$	$\dots$	$(k,0)$
$\vdots$	$\vdots$			$\vdots$	$\vdots$			$\vdots$
$(2k,1)$	$(1+2k,1)$	$(2+2k,1)$	$\dots$	$(\frac{5k-1}{2},1)$	$(-2k,0)$	$(1-2k,0)$	$\dots$	$(\frac{k-1}{2}-2k,0)$
$(k,1)$	$(1+k,1)$	$(2+k,1)$	$\dots$	$(\frac{3k-1}{2},0)$	$(-k,0)$	$(1-k,0)$	$\dots$	$(\frac{k-1}{2}-k,0)$

Table 1: Addition table of S and T in D_{2n} with the quadrants highlighted

We now show that every element of $\mathbb{Z}_n \rtimes \mathbb{Z}_3$ appears precisely once in this table. Note that

$$|S||T| = (\frac{k-1}{2} + \frac{k-1}{2} + 1)(\frac{\alpha-1}{2} + 1 + \frac{\alpha-1}{2}) = k \cdot \alpha = 2n-1$$

Hence, we need only show that each element appears at least once in Table 1.
We divide the table into the quadrants highlighted in Table 1:

$$\Delta_1 = \{(\lambda + \mu k, 0) : 1 \leq \lambda \leq \frac{k-1}{2}, 0 \leq \mu \leq \frac{\alpha-1}{2}\}$$

$$\Delta_2 = \{(\xi - \lambda k, 1) : 0 \leq \xi \leq \frac{k-1}{2}, 1 \leq \mu \leq \frac{\alpha-1}{2}\}$$

$$\Delta_3 = \{(\lambda + \pi k, 1) : 1 \leq \lambda \leq \frac{k-1}{2}, 1 \leq \pi \leq \frac{\alpha-1}{2}$$

$$\Delta_4 = \{(\xi - \pi k, 0) : 0 \leq \xi \leq \frac{k-1}{2}, 1 \leq \pi \leq \frac{\alpha-1}{2}\}$$

Within each block, across the row we add one to the $\mathbb{Z}_n$ component, whilst keeping the $\mathbb{Z}_3$ component constant. Down the columns of Δ_1 and Δ_3, we add k to the $\mathbb{Z}_n$ component, and subtract k down the columns of Δ_2 and Δ_4.

Hence, looking at the top rows of Δ_1 and Δ_4, we have

$$(1,0), (2,0), \dots (\frac{k-1}{2}, 0), (\frac{k+1}{2}, 0), (1 + \frac{k+1}{2}, 0) \dots (k, 0)$$

. Then similarly with the second rows of Δ_1 and second Δ_4, we get

$$(1+k,0),(2+k,0)\dots(k+\frac{k-1}{2},0),(k+\frac{k+1}{2},0),\dots(2k,0)$$

and so on. There is one less row in Δ_4 than in Δ_1 so the pattern finishes on the last row of Δ_1 with

$$(1+n-\frac{k+1}{2},0),\dots,(n-1,0)$$

This gives us every element of the form $(x,0)$ where $x \in \mathbb{Z}_n$.

We see a similar pattern in Δ_2 and Δ_3. Taking the top and bottom row of Δ_2, we have

$$(0,1),(1,1),\dots,(\frac{k-1}{2},1)(\frac{k+1}{2},1),(1+\frac{k+1}{2}),\dots,(k,1)$$

Then the bottom row of Δ_3 and second bottom row of Δ_2 gives,

$$(1+k,1),(2+k),\dots,(k+\frac{k-1}{2},1),(k+\frac{k+1}{2},1),\dots,(2k,1)$$

This pattern continues which gives us every element of the form $(x,1)$ where $x \in \mathbb{Z}_n$. Hence, every element appears precisely once in Table 1, and so (S,T) is a near factorisation of D_{2n} □

So now we can explain all the GSEDFs with parameters $(v,2;k_1,k_2;1,1)$ where $v = k_1k_2+1$, in both the cyclic and dihedral group of each order. In fact, the computational data suggests that this construction is only valid within these groups. Theorem 2.9 also gives us a useful way of converting from a direct product with $\mathbb{Z}_2$ to the analogous semidirect product. This then leads to the question: is this process possible when taking the semidirect product with a different group. Here we will look at $\mathbb{Z}_3$.

A semidirect product $\mathbb{Z}_n \rtimes \mathbb{Z}_3$ requires an automorphism of order 3 in $Aut(\mathbb{Z}_n)$. $Aut(\mathbb{Z}_n)$ is isomorphic to the set of units (elements that have an multiplicative inverse) in $\mathbb{Z}_n$.

Remark Here we are considering $\mathbb{Z}_n$ under both addition and multiplication, and so, for the rest of this section, we think of $\mathbb{Z}_n$ as a ring rather than a group.

Any automorphism in $Aut(\mathbb{Z}_n)$ can be defined as multiplication by a unit element. So, an order 3 automorphism is equivalent to multiplication by a

unit of order 3 in the group of units of $\mathbb{Z}_n$, which we denote $\mathbb{Z}_n^\times$. Recall from Chapter 1.2, that the order of an element must divide the order of the group; this places restrictions on which groups may have an order 3 automorphism. When n is prime, $\mathbb{Z}_n^\times$ has order $n-1$, as only 0 is not a unit. Therefore, we require $3|n-1$ or equivalently, $n \equiv 1 \; mod \; 3$. For a general (not necessarily prime) n, $|\mathbb{Z}_n^\times| = \phi(n)$ so we require $3|\phi(n)$.

Let α an order 3 unit in $\mathbb{Z}_n$. Then, let Y be a subset of $\mathbb{Z}_n \times \mathbb{Z}_3$ such that $\alpha Y = Y$. We first prove the following lemmas.

Lemma 2.13. Suppose α is an order 3 unit of $\mathbb{Z}_n$, and $Y \subseteq \mathbb{Z}_n \times \mathbb{Z}_3$ s.t $\alpha Y = Y$. Then, if $\alpha \equiv 0 \; mod \; 3$, for all $(y_1, y_2) \in Y$, $y_2 = 0$.

Proof. Since $\alpha Y = Y$, for all $(y_1, y_2) \in Y$ there exists $(z_1, z_2) \in Y$ such that $(y_1, y_1) = \alpha(z_1, z_2) = (\alpha z_1, \alpha z_2)$. Hence $y_2 = \alpha z_2 \equiv 0 \cdot z_2 = 0 \; mod \; 3$. □

Lemma 2.14. Suppose α is an order 3 unit of $\mathbb{Z}_n$, and $Y \subseteq \mathbb{Z}_n \times \mathbb{Z}_3$ s.t $\alpha Y = Y$. Then for all $(y_1, y_2) \in Y$, $\alpha^2(y_1, y_2) = (\alpha^2 y_1, y_2)$.

Proof. If $\alpha \equiv 1 \; mod \; 3$, then $\alpha z \equiv z \; mod \; 3$ for all $z \in \mathbb{Z}_3$. Therefore, $\alpha^2 z = \alpha(\alpha z) \equiv \alpha z \equiv z \; mod \; 3$. Hence $\alpha^2(y_1, y_2) = (\alpha^2 y_1, \alpha^2 y_2) = (\alpha^2 y_1, y_2)$ If $\alpha \equiv 2 \; mod \; 3$, then $\alpha^2 \equiv 2^2 = 4 \equiv 1 \; mod \; 3$. Hence, $\alpha^2 z \equiv z \; mod \; 3$. Therefore, $\alpha^2(y_1, y_2) = (\alpha^2 y_1, \alpha^2 y_2) = (\alpha^2 y_1, y_2)$. If $\alpha \equiv 0 \; mod \; 3$, then Lemma 2.13 tells us that $y_2 = 0$, and so $\alpha^2(y_1, y_2) = \alpha^2(y_1, 0) = (\alpha^2 y_1, 0) = (\alpha^2 y_1, y_2)$. □

These two Lemmas give us the following facts.

Corollary 2.15. Suppose α is an order 3 unit of $\mathbb{Z}_n$, and $Y \subseteq \mathbb{Z}_n \times \mathbb{Z}_3$ s.t $\alpha Y = Y$. Then, for all $(y_1, y_2) \in Y, (\alpha^2 y_1, y_2) \in Y$.

Proof. $\alpha Y = Y \implies \alpha^2 Y = \alpha(\alpha Y) = \alpha Y = Y$. So, if $(y_1, y_2) \in Y$, then $\alpha^2(y_1, y_2) \in Y$ and, from Lemma 2.14, $\alpha^2(y_1, y_2) = (\alpha^2 y_1, y_2)$. □

Corollary 2.16. Suppose α is an order 3 unit of $\mathbb{Z}_n$, and $Y \subseteq \mathbb{Z}_n \times \mathbb{Z}_3$ s.t $\alpha Y = Y$. Then, for all $(y_1, y_2) \in Y, (\alpha y_1, y_2) = (\alpha y_1, y_2) \in Y$.

Proof. In the proof of Corollary 2.15 we saw that $\alpha Y = Y \implies \alpha^2 Y = Y$. Hence, $\alpha^4 Y = \alpha^2(\alpha^2 Y) = \alpha^2 Y = Y$. So, if $(y_1, y_2) \in Y$, then $\alpha^4(y_1, y_2) \in Y$. $\alpha^4(y_1, y_2) = \alpha^2(\alpha^2(y_1, y_2))$ so by applying Lemma 2.14 twice we get $\alpha^4(y_1, y_2) = \alpha^2(\alpha^2 y_1, y_2) = (\alpha^4 y_1, y_2) \in Y$. Since $\alpha^3 = 1$ in $\mathbb{Z}_n$, so $\alpha^4 = \alpha$, we have $(\alpha y_1, y_2) = (\alpha^4 y_1, y_2) \in Y$. □

Now, using these two facts we can prove a theorem similar to Theorem 2.9 but using $\mathbb{Z}_3$ in place of $\mathbb{Z}_2$.

Theorem 2.17. Let $\mathbb{Z}_n$ be a ring with operation $*_n$, where $3|\phi(n) = |\mathbb{Z}_n^\times|$. Define $\mathbb{Z}_3 = \{0, 1, 2\}$ with addition denoted $*_3$.

Let α be an order 3 element of $\mathbb{Z}_n^\times$. Define the homomorphism $\Gamma : \mathbb{Z}_3 \to Aut(\mathbb{Z}_n)$ by

$$\Gamma(x) = \phi_x, \text{ for all } x \in \mathbb{Z}_3, \text{ where } \phi_x(y) = \alpha^x y \text{ mod n for all } y \in \mathbb{Z}_n$$

Denote by $*$ the operation in $\mathbb{Z}_n \times \mathbb{Z}_3$, and by $*_\Gamma$ the operation in the semidirect product $\mathbb{Z}_n \rtimes \mathbb{Z}_3$ defined by Γ.

Then, if $X, Y \subseteq \mathbb{Z}_n \times \mathbb{Z}_3$ such that $\alpha X = X$ and $\alpha Y = Y$, $X *_\Gamma Y = X * Y$.

Proof. Let (x_1, x_2) be an element of X with multiplicity $\mu_X((x_1, x_2))$, and similarly let (y_1, y_2) be an element of Y with multiplicity $\mu_Y((y_1, y_2))$. Then $(x_1, x_2) *_\phi (y_1, y_2) \in X *_\phi Y$.

We first show $X *_\phi Y \subseteq X * Y$, and
$\mu_{X*_\phi Y}((x_1, x_2) *_\phi (y_1, y_2)) \leq \mu_{X*Y}((x_1, x_2) * (y_1, y_2))$.

If $x_2 = 0$:

$$\begin{aligned}(x_1, x_2) *_\Gamma (y_1, y_2) &= (x_1 *_n \phi_0(y_1), x_2 *_3 y_2) \\ &= (x_1 *_n y_1, x_2 *_3 y_2) \\ &= (x_1, x_2) * (y_1, y_2) \in X * Y\end{aligned}$$

If $x_2 = 1$:

$$\begin{aligned}(x_1, x_2) *_\Gamma (y_1, y_2) &= (x_1 *_n \phi_1(y_1), x_2 *_3 y_2) \\ &= (x_1 *_n \alpha y_1, x_2 *_3 y_2) \\ &= (x_1, x_2) * (\alpha y_1, y_2) \in X * Y \text{ by Corollary 2.16}\end{aligned}$$

If $x_2 = 2$:

$$\begin{aligned}(x_1, x_2) *_\Gamma (y_1, y_2) &= (x_1 *_n \phi_2(y_1), x_2 *_3 y_2) \\ &= (x_1 *_n \alpha^2 y_1, x_2 *_3 y_2) \\ &= (x_1, x_2) * (\alpha^2 y_1, y_2) \in X * Y \text{ by Corollary 2.15.}\end{aligned}$$

So $(x_1, x_2) *_\Gamma (y_1, y_2) \in X * Y$, and so $X *_\Gamma Y \subseteq X * Y$.

For the latter statement, $\mu_X(x) \leq \mu_X(x)$ and $\mu_Y(y) \leq \mu_Y(y)$. Hence, since multiplicities are positive integers:

$$\begin{aligned}\mu_{X*_\phi Y}((x_1,x_2) *_\phi (y_1,y_2)) &= \mu_X((x_1,x_2)) \cdot \mu_Y((y_1,y_2)) \text{ by Lemma 2.10} \\ &\leq \mu_X((x_1,x_2)) \cdot \mu_Y((y_1,y_2)) \text{ from above} \\ &= \mu_{X*Y}((x_1,x_2) * (y_1,y_2)) \text{ by Lemma 2.10}\end{aligned}$$

Conversely, we show $X * Y \subseteq X *_\Gamma Y$, and
$\mu_{X*_\phi Y}((x_1,x_2) *_\phi (y_1,y_2)) \geq \mu_{X*Y}((x_1,x_2) * (y_1,y_2))$:

If $x_2 = 0$:

$$\begin{aligned}(x_1,x_2) * (y_1,y_2) &= (x_1 *_n y_1, x_2 *_3 y_2) \\ &= (x_1 *_n \phi_0(y_1), x_2 *_3 y_2) \\ &= (x_1,x_2) *_\Gamma (y_1,y_2) \in X *_\Gamma Y\end{aligned}$$

If $x_2 = 1$:

$$\begin{aligned}(x_1,x_2) * (y_1,y_2) &= (x_1 *_n y_1, x_2 *_3 y_2) \\ &= (x_1 *_n \alpha^3 y_1, x_2 * y_2) \\ &= (x_1 *_n \phi_1(\alpha^2 y_1), x_2 *_3 y_2) \\ &= (x_1,x_2) *_\Gamma (\alpha^2 y_1, y_2) \in X *_\Gamma Y \text{ by Corollary 2.15}\end{aligned}$$

If $x_2 = 2$:

$$\begin{aligned}(x_1,x_2) * (y_1,y_2) &= (x_1 *_n y_1, x_2 *_3 y_2) \\ &= (x_1 *_n \alpha^3 y_1, x_2 * y_2) \\ &= (x_1 *_n \phi_2(\alpha y_1), x_2 *_3 y_2) \\ &= (x_1,x_2) *_\Gamma (\alpha y_1, y_2) \in X *_\Gamma Y \text{ by Corollary 2.16}\end{aligned}$$

So $(x_1,x_2) * (y_1,y_2) \in X *_\Gamma Y$ for all $(x_1,x_2) \in X, (y_1,y_2) \in Y$.

Again, for the latter statement, $\mu_X(x) \leq \mu_X(x)$ and $\mu_Y(y) \leq \mu_Y(y)$. Hence, since multiplicities are positive integers:

$$\begin{aligned}\mu_{X*Y}((x_1,x_2) * (y_1,y_2)) &= \mu_X((x_1,x_2)) \cdot \mu_Y((y_1,y_2)) \text{ by Lemma 2.10} \\ &\leq \mu_X((x_1,x_2)) \cdot \mu_Y((y_1,y_2)) \text{ from above} \\ &= \mu_{X*_\phi Y}((x_1,x_2)_\phi * (y_1,y_2)) \text{ by Lemma 2.10}\end{aligned}$$

So $\mu_{X*_\phi Y}((x_1,x_2) *_\phi (y_1,y_2)) = \mu_{X*Y}((x_1,x_2) * (y_1,y_2))$ and so $X *_\Gamma Y = X * Y$. □

Example 2.18. There is a $(12, 19)$ 6-fold near-factorisation in $\mathbb{Z}_{39}$ given by

$$\{0, 1, 2, 3, 4, 7, 8, 9, 10, 11, 15, 19, 21, 24, 25, 26, 29, 31, 35\}$$

$$\{3, 6, 7, 9, 12, 16, 19, 21, 22, 25, 33, 34\}$$

Writing this as ordered pairs in $\mathbb{Z}_{13} \times \mathbb{Z}_3 \cong \mathbb{Z}_{39}$ gives,

$$X = \{(3,0), (6,0), (7,1), (9,0), (12,0), (3,1), (6,1), (8,0), (9,1), (12,1), (7,0),$$
$$(8,1)\}$$
$$Y = \{(0,0), (1,1), (2,2), (3,0), (4,1), (7,1), (8,2), (9,0), (10,1), (11,2), (2,0),$$
$$(6,1), (8,0), (11,0), (12,1), (0,2), (3,2), (5,1), (9,2)\}$$

The semidirect product $\mathbb{Z}_{13} \rtimes \mathbb{Z}_3$ is defined by the homomorphism $\phi_x(y) = 9y$, so we want our sets to have the property $X = 9X$ and $Y = 9Y$. Adding $(1, 0)$ to X and subtracting this from Y gives the equivalent near factorisation (X', Y').

$$X' = \{(2,0), (5,0), (6,1), (8,0), (11,0), (2,1), (5,1), (7,0), (8,1), (11,1),$$
$$(6,0), (7,1)\}$$
$$Y' = \{(1,0), (2,1), (3,2), (4,0), (5,1), (8,1), (9,2), (10,0), (11,1), (12,2),$$
$$(3,0), (7,1), (9,0), (12,0), (0,1), (1,2), (4,2), (6,1), (10,2)\}$$

Which is a $(12, 19)$ 6-fold near-factorisation of $\mathbb{Z}_{13} \rtimes \mathbb{Z}_3$.

However, in certain groups we observe a similar pattern of a GSEDF existing in both the direct and semidirect product, yet Theorem 2.17 cannot be applied as the $Y = \alpha Y$ condition can never be satisfied.

Example 2.19. There is a $(4, 10)$ 2-fold near-factorisation in $\mathbb{Z}_{21}$ given by

$$\{1, 8, 10, 17\}$$

$$\{0, 1, 2, 3, 5, 6, 8, 16, 18, 19\}$$

Which written as ordered pairs in $\mathbb{Z}_7 \times \mathbb{Z}_3$ is

$$X = \{(1,1), (1,2), (3,1), (3,2)\}$$

$$Y = \{(0,0), (1,1), (2,2), (3,0), (5,2), (6,0), (1,2), (2,1), (4,0), (5,1)\}$$

The semidirect product $\mathbb{Z}_7 \rtimes \mathbb{Z}_3$ is defined by the homomorphism $\phi_x(y) = 4y$, so we want our sets to have the property $X = 4X$ and $Y = 4Y$. The $\mathbb{Z}_3$ component will always remain fixed under multiplication by $4 \equiv 1 \ mod\ 3$. However, since 4 is an order 3 element of $\mathbb{Z}_7$ no element aside for 0 maps to itself, and no two elements can be 'swapped'. Consequently, since there are only two different $\mathbb{Z}_7$ components in X, it is not possible to add a constant to X and reach a set X' such that $X' = 4X'$.

Example 2.19 shows that the idea presented in Theorem 2.17 does not explain every case where we appear to be transforming between the direct and semidirect product.

3 Recursive Constructions for $m = 2$

In this section we provide a more detailed proof for Construction 4.5 in [10], and then consider how this construction can be adapted for semidirect products in the special case $t = 3$.

Theorem 3.1. [10](Construction 4.5) Let $v > 1, t > 1$ and $v \equiv t \equiv 1 \pmod 2$. Let G be a group of order v. If there exists a $(v, 2; 2\lambda, \frac{v-1}{2}; \lambda, \lambda)$-GSEDF in G, then there exists a $(vt, 2; 4\lambda, \frac{vt-1}{2}; 2\lambda, 2\lambda)$-GSEDF in $G \times \mathbb{Z}_t$.

Proof. Suppose $\{D_1, D_2\}$ is a $(v, 2; 2\lambda, \frac{v-1}{2}; 2\lambda, 2\lambda)$-GSEDF in the group G with identity 0. Then $|D_1| = 2\lambda, |D_2| = \frac{v-1}{2}$ and $\Delta(D_1, D_2) = \Delta(D_2, D_1) = \lambda(G \backslash \{0\})$. Let

$$D_1' = \{(x, j) : x \in D_1, j = 0, 1\}$$

$$D_2' = \{(x, 0), (x, 2i-1) : x \in D_2, 1 \leq i \leq \frac{t-1}{2}\} \cup$$

$$\{(y, 2i) : y \in G \backslash D_2, 1 \leq i \leq \frac{t-1}{2}\}$$

We will show $\{D_1', D_2'\}$ is a $(vt, 2; 4\lambda, \frac{vt-1}{2}; 2\lambda, 2\lambda)$-GSEDF in $G \times \mathbb{Z}_t$.

First, check $D_1', D_2' \subset G \times \mathbb{Z}_t$:

$D_1 \subset G$ and $\{0, 1\} \subset \mathbb{Z}_t$ as $t > 1$, so $D_1' \subset G \times \mathbb{Z}_t$.

$D_2' \subset G$ and $0 \in \mathbb{Z}_t$, so $(x, 0) \in G \times \mathbb{Z}_t \ \forall x \in D_2$, $1 \leq i \leq \frac{t-1}{2}$

$\implies 1 \leq 2i - 1 \leq t - 2 \implies 2i - 1 \in \mathbb{Z}_t$ for all $1 \leq i \leq \frac{t-1}{2}$.

So $\{(x, 0), (x, 2i-1) : x \in D_2, 1 \leq i \leq \frac{t-1}{2}\} \subseteq G \times \mathbb{Z}_t$.

For all $x \in D_2, (x, t-1) \notin \{(x, 0), (x, 2i-1) : x \in D_2, 1 \leq i \leq \frac{t-1}{2}\}$.

So $\{(x,0),(x,2i-1) : x \in D_2, 1 \leq i \leq \frac{t-1}{2}\} \subset G \times \mathbb{Z}_t$.
Also, $G\backslash D_2 \subset G$, and $\{2i; 1 \leq i \leq \frac{t-1}{2}\} \subset \mathbb{Z}_t$ as $2 \leq 2i \leq t-1$.
So $\{(y,2i) : y \in G\backslash D_2, 1 \leq i \leq \frac{t-1}{2}\} \subset G \times \mathbb{Z}_t$.
Hence, $D_2' = \{(x,0),(x,2i-1) : x \in D_2, 1 \leq i \leq \frac{t-1}{2}\} \cup$
$\{(y,2i) : y \in G\backslash D_2, 1 \leq i \leq \frac{t-1}{2}\} \subset G \times \mathbb{Z}_t$.

Now we check D_1' and D_2' are disjoint:
Suppose $(x_1,x_2) \in D_1' \cap D_2'$.
Then $(x_1,x_2) \in D_1'$ so $x_1 \in D_1$ and $x_2 = 0, 1$.
$x_1 \in D_1 \implies x_1 \notin D_2$ so, since $(x_1,x_2) \in D_2'$, we must have $x_1 \in G\backslash D_2$.
Hence, $x_2 = 2i$ for some $1 \leq i \leq \frac{t-1}{2} \implies 2 \leq x_2 \leq t-1$, which contradicts $(x_1,x_2) \in D_1'$.
Therefore, $D_1' \cap D_2' = \phi$

Check the sizes of D_1' and D_2':
$D_1' \cong D_1 \times \mathbb{Z}_2$ so $|D_1'| = |D_1| \cdot |\mathbb{Z}_2| = 2\lambda \cdot 2 = 4\lambda$
In D_2' there are $|D_2|$ options for x, $|G\backslash D_2|$ options for y, and $\frac{t-1}{2}$ options for i.
Hence $|D_2'| = |\{(x,0),(x,2i-1) : x \in D_2, 1 \leq i \leq \frac{t-1}{2}\}| + |\{(y,2i); y \in G\backslash D_2 : y \in G\backslash D_2, 1 \leq i \leq \frac{t-1}{2}\}| = |D_2|(1+\frac{t-1}{2}) + |G\backslash D_2|\frac{t-1}{2} = \frac{v-1}{2}(1+\frac{t-1}{2}) + (v-\frac{v-1}{2})\frac{t-1}{2} = \frac{v-1}{2} + \frac{vt-v}{v} = \frac{vt-1}{2}$

Now we consider $\Delta(D_2', D_1')$. Let

$$D_1 = \{a_1, a_2, \ldots, a_l\},$$

$$D_2 = \{b_1, b_2, \ldots, b_m\}$$

$$G\backslash(D_1 \cup D_2) = \{c_1, c_2, \ldots, c_n\}$$

where $l = 2\lambda, m = \frac{v-1}{2}$ and $n = \frac{v+1}{2} - 2\lambda$. Then we can write

$$\Delta(D_2', D_1') = \Delta_1 \cup \Delta_2 \cup \Delta_3$$

where

$$\Delta_1 = \{(x,0),(x,-1) : x \in \Delta(D_2, D_1)\}$$

$$\Delta_2 = \{(x,2i-1),(x,2i-2) : x \in \Delta(D_2, D_1), 1 \leq\ i \leq \frac{t-1}{2}\}$$

$$\Delta_3 = \{(y,2i),(y,2i-1) : y \in \Delta(G\backslash D_2, D_1), 1 \leq i \leq \frac{t-1}{2}\}$$

This can be represented with the following subtraction table where the above blocks are highlighted:

	$(a_1,0)$	$\dots$	$(a_l,0)$	$(a_1,1)$	$\dots$	$(a_l,1)$
$(b_1,0)$	$(b_1-a_1,0)$	$\dots$	$(b_1-a_l,0)$	$(b_1-a_1,-1)$	$\dots$	$(b_1-a_l,-1)$
$\vdots$	$\vdots$		$\vdots$	$\vdots$		$\vdots$
$(b_m,0)$	$(b_m-a_1,0)$	$\dots$	$(b_m-a_l,0)$	$(b_m-a_1,-1)$	$\dots$	$(b_m-a_l,-1)$
$(b_1,1)$	$(b_1-a_1,1)$	$\dots$	$(b_1-a_l,1)$	$(b_1-a_1,0)$	$\dots$	$(b_1-a_l,0)$
$\vdots$	$\vdots$		$\vdots$	$\vdots$		$\vdots$
$(b_1,t-2)$	$(b_1-a_1,t-2)$	$\dots$	$(b_1-a_l,t-2)$	$(b_1-a_1,t-3)$	$\dots$	$(b_1-a_l,t-3)$
$(b_2,1)$	$(b_2-a_1,1)$	$\dots$	$(b_2-a_l,1)$	$(b_2-a_1,0)$	$\dots$	$(b_2-a_l,0)$
$\vdots$	$\vdots$		$\vdots$	$\vdots$		$\vdots$
$(b_m,t-2)$	$(b_m-a_1,t-2)$	$\dots$	$(b_m-a_l,t-2)$	$(b_m-a_1,t-3)$	$\dots$	$(b_m-a_l,t-3)$
$(a_1,2)$	$(0,2)$	$\dots$	$(a_1-a_l,2)$	$(0,1)$	$\dots$	$(a_1-a_l,1)$
$\vdots$	$\vdots$		$\vdots$	$\vdots$		$\vdots$
$(a_1,t-1)$	$(0,t-1)$	$\dots$	$(a_1-a_l,t-1)$	$(0,t-2)$	$\dots$	$(a_1-a_l,t-2)$
$(a_2,2)$	$(a_2-a_1,2)$	$\dots$	$(a_2-a_l,2)$	$(a_2-a_1,1)$	$\dots$	$(a_2-a_l,1)$
$\vdots$	$\vdots$		$\vdots$	$\vdots$		$\vdots$
$(a_l,t-1)$	$(a_l-a_1,t-1)$	$\dots$	$(0,t-1)$	$(a_l-a_1,t-2)$	$\dots$	$(0,t-2)$
$(c_1,2)$	$(c_1-a_1,2)$	$\dots$	$(c_1-a_l,2)$	$(c_1-a_1,1)$	$\dots$	$(c_1-a_l,1)$
$\vdots$	$\vdots$		$\vdots$	$\vdots$		$\vdots$
$(c_1,t-1)$	$(c_1-a_1,t-1)$	$\dots$	$(c_1-a_l,t-1)$	$(c_1-a_1,t-2)$	$\dots$	$(c_1-a_l,t-2)$
$(c_2,2)$	$(c_2-a_1,2)$	$\dots$	$(c_2-a_l,2)$	$(c_2-a_1,1)$	$\dots$	$(c_2-a_l,1)$
$\vdots$	$\vdots$		$\vdots$	$\vdots$		$\vdots$
$(c_n,t-1)$	$(c_n-a_1,t-1)$	$\dots$	$(c_n-a_l,t-1)$	$(c_n-a_1,t-2)$	$\dots$	$(c_n-a_l,t-2)$

Table 2: The subtraction table for the $(vt,2;4\lambda,\frac{vt-1}{2};2\lambda,2\lambda)$-GSEDF in $G\times\mathbb{Z}_t$, constructed with the above method.

Now we show $\Delta(D_1', D_1') = 2\lambda((G \times (Z)_t)\backslash\{0\})$. To do this, we show every element $(a, b) \in (G \times \mathbb{Z}_t)\backslash\{0\}$ appears exactly two times in $\Delta(D_2', D_1')$ Note that $|D_1'||D_2'| = 4\lambda(\frac{vt-1}{2}) = 2\lambda(vt-1) = 2\lambda|(G \times \mathbb{Z}_t)\backslash\{0\}|$. Hence, it is sufficient to show that every element $(a, b) \in (G \times \mathbb{Z}_t)\backslash\{0\}$ appears at least 2λ times. To do this we observe the following things:

1. $\Delta(D_2, D_1) = \lambda(G\backslash\{0\})$ as $\{D_1, D_2\}$ is a GSEDF in G.
2. $\Delta(G\backslash D_2, D_1) = 2\lambda\{0\} + \lambda(G\backslash\{0\})$. We can see this from the subtraction table:

	a_1	$\dots$	a_l
a_1	0	$\dots$	$a_l - a_1$
$\vdots$	$\vdots$		$\vdots$
a_l	$a_1 - a_l$	$\dots$	0
c_1	$a_1 - c_1$	$\dots$	$a_l - c_1$
$\vdots$	$\vdots$		$\vdots$
c_l	$a_1 - c_l$	$\dots$	$a_l - c_l$

   Here 0 occurs $|D_1| = 2\lambda$ times.
   Also $\Delta(G\backslash D_2, D_1) = \Delta(G, D_1) - \Delta(D_2, D_1) = |D_1|G - \lambda(D\backslash\{0\}) = 2\lambda\{0\} + 2\lambda(G\backslash\{0\}) - \lambda(G\backslash\{0\}) = 2\lambda\{0\} + \lambda(G\backslash\{0\})$

Consider the following cases:

- Case 1: $b = 0$:
  When $b = 0, a \neq 0$ as $D_1' \cap D_2' = \phi$, so $(0, 0) \notin \Delta(D_2', D_1')$. So for any $a \in G$, by **1**, $(a, 0)$ appears λ times in Δ_1. Also, we see $(a, 0)$ λ times in Δ_2 from setting $i = 1$ in the $(x, 2i-2)$ component.
- Case 2: $b \equiv 1 \ mod\ 2$:
  - Case 2.1: $a \neq 0$:
    $b \equiv 1 \ mod\ 2$ and $b \in \mathbb{Z}_t \implies b = 2i - 1$ where $1 \leq i \leq \frac{t-1}{2}$ so for any $a \in G\backslash\{0\}$ and $b \in \mathbb{Z}_t$ such that $b \equiv 1 \pmod 2$, $(a, b) = (a, 2i-1)$ for some $1 \leq i \leq \frac{t-1}{2}$. By **1**, $(a, 2i-1)$ appears λ times in Δ_2 and λ times in Δ_3 by **2**.
  - Case 2.2: $a = 0$:
    $0 \notin \Delta(D_2, D_1)$ so $(0, b)$ only appears in Δ_3. From **1**, $(0, b)$ appears 2λ times in Δ_3.

- Case 3: $b \equiv 0 \ mod\ 2$ and $b \neq 0$:
  - Case 3.1: $a \neq 0$:
    $b \equiv 0 \ mod\ 2$, $b \neq 0$ and $b \in \mathbb{Z}_t \implies b = 2i-2$ for $2 \leq i \leq \frac{t-1}{2}$, or $b = 2i, 1 \leq i \leq \frac{t-1}{2}$.$(a, 2i-2)$ appears λ times in Δ_2 by **1**, and $(a, 2i)$ appears λ times in Δ_3 by **2**. Hence, (a, b) where $a, b \neq 0$ and $b \equiv 0 \ mod\ 2$, appears 2λ times.
  - Case 3.2: $a = 0$:
    From **2**, given any $b \equiv 0 \ mod\ 2$, (a, b) appears 2λ times in Δ_3.

Hence, every element $(a, b) \in (G \times \mathbb{Z}_t) \backslash \{0\}$ appears exactly 2λ times in $\Delta(D_2', D_1')$. So $\Delta(D_2', D_1') = 2\lambda((G \times \mathbb{Z}_t) \backslash \{0\})$, and therefore $\{D_1', D_2'\}$ is a $(vt, 2; 4\lambda, \frac{vt-1}{2}; 2\lambda, 2\lambda)$-GSEDF in $G \times \mathbb{Z}_t$. □

Example 3.2. There exists a $(7, 2; 2, 3; 1, 1)$-GSEDF in $\mathbb{Z}_7$ given by

$$D_1 = \{0, 1\}, D_2 = \{2, 4, 6\}.$$

Using the method from the proof of Theorem 3.1, we can construct

$$D_1' = \{(0,0), (0,1), (1,0), (1,1)\}$$

$$D_2' = \{(2,0), (4,0), (6,0), (2,1), (4,1), (6,1), (0,2), (1,2), (3,2), (5,2)\}.$$

Looking at the following table representing $\Delta(D_2', D_1')$, we can see that $\{D_1', D_2'\}$ is a $(21, 2; 4, 10; 2, 2)$- GSEDF in $\mathbb{Z}_{21}$.

	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(2,0)$	$(5,0)$	$(5,1)$	$(6,0)$	$(6,1)$
$(4,0)$	$(3,0)$	$(3,1)$	$(4,0)$	$(4,1)$
$(6,0)$	$(1,0)$	$(1,1)$	$(2,0)$	$(2,1)$
$(2,1)$	$(5,2)$	$(5,0)$	$(6,2)$	$(6,1)$
$(4,1)$	$(3,2)$	$(3,0)$	$(4,2)$	$(4,0)$
$(6,1)$	$(1,2)$	$(1,0)$	$(2,2)$	$(2,0)$
$(0,2)$	$(0,1)$	$(0,2)$	$(1,1)$	$(1,2)$
$(1,2)$	$(6,1)$	$(6,2)$	$(0,1)$	$(0,2)$
$(3,2)$	$(4,1)$	$(4,2)$	$(5,1)$	$(5,2)$
$(5,2)$	$(2,1)$	$(2,2)$	$(3,1)$	$(3,2)$

Table 3: $\Delta(D_2', D_1')$ with the blocks highlighted as in the proof of Theorem 3.1

This GSEDF is equivalent to the GSEDF derived from the near factorisation given in Example 2.19.

Theorem 3.1 tells us that, given any $(v, 2; 2\lambda, \frac{v-1}{2}; \lambda, \lambda)$ GSEDF in $\mathbb{Z}_v$ where $v > 1$ and $v \equiv 1 \ mod \ 2$, we can contruct a GSEDF in $\mathbb{Z}_v \times \mathbb{Z}_t$ with parameters $(vt, 2; 4\lambda, \frac{vt-1}{2}; 2\lambda, 2\lambda)$ for $t > 1, t \equiv 1 \ mod \ 2$. However, in every example we found of these 'larger' GSEDFs we also found a GSEDF with the same parameters in the semidirect product $\mathbb{Z}_v \rtimes \mathbb{Z}_3$. Hence, we ask the question, does a similar recursive construction exist to build these GSEDFs in the semidirect product?

In the case where $t = 3$, if, by adding a constant if necessary, the GSEDF constructed in the direct product using the method in Theorem 3.1, satisfies the conditions in Theorem 2.17, then we may use the same construction and convert with ease between direct and semidirect product.

Example 3.3. There exists a $(13, 3; 6, 6; 3, 3)$-GSEDF in $\mathbb{Z}_{13}$ given by

$$D_1 = \{0, 1, 2, 3, 6, 10\}, D_2 = \{4, 5, 7, 9, 11, 12\}$$

Applying Theorem 3.1 we can construct a $(39, 2; 12, 19; 6, 6)$-GSEDF in $\mathbb{Z}_{13} \times \mathbb{Z}_3$.

$$D_1' = \{(0,0), (0,1), (1,0), (1,1), (2,0), (2,1), (3,0), (3,1), (6,0), (6,1),$$
$$(10,0), (10,1)\}$$
$$D_2' = \{(4,0), (5,0), (7,0), (9,0), (11,0), (12,0), (4,1), (5,1), (7,1), (9,1),$$
$$(11,1), (12,1), (0,2), (1,2), (2,2), (3,2), (6,2), (8,2), (10,2)\}$$

Adding $(6, 0)$ to D_1' and D_2' gives

$$D_1' = \{(6,0), (6,1), (7,0), (7,1), (8,0), (8,1), (9,0), (9,1), (12,0), (12,1),$$
$$(3,0), (3,1)\}$$
$$D_2' = \{(10,0), (11,0), (0,0), (2,0), (4,0), (5,0), (10,1), (11,1), (0,1), (2,1),$$
$$(4,1), (5,1), (6,2), (7,2), (8,2), (9,2), (12,2), (1,2), (3,2)\}$$

This is the GSEDF equivalent to the $(12, 19)$ 6-fold near factorisation we saw in Example 2.18. To verify this, we observe that $D_1' = X$ and then one simply needs to invert D_2' to check this is equivalent to Y. Therefore, following Example 2.18 we can add $(0, 1)$ to D_1' and D_2', which then gives a $(39, 2; 12, 19; 6, 6)$-GSEDF in $\mathbb{Z}_{13} \rtimes \mathbb{Z}_3$.

However, we saw in Example 2.19 that, in a large number of cases, it is impossible to satisfy the conditions needed to apply Theorem 2.17. Therefore, we know that the recursive construction from Theorem 3.1 cannot always be used to construct the corresponding GSEDF in the semidirect product as we did above in Example 3.3.

Example 3.4. There exists a $(21, 2; 4, 10; 2, 2)$-GSEDF in $\mathbb{Z}_7 \rtimes \mathbb{Z}_3$ given by

$$D_1 = \{(3,1), (3,2), (5,1), (4,2)\}$$

$$D_2 = \{(0,1), (4,1), (1,1), (0,2), (2,2), (5,2), (0,0), (1,0), (2,0), (3,0)\}$$

Consider the subtraction table for this GSEDF:

	$(3,1)$	$(3,2)$	$(5,1)$	$(4,2)$
$(0,1)$	$(3,0)$	$(3,1)$	$(5,0)$	$(4,1)$
$(4,1)$	$(6,0)$	$(1,1)$	$(1,0)$	$(2,1)$
$(1,1)$	$(2,0)$	$(6,1)$	$(4,0)$	$(0,1)$
$(0,2)$	$(3,2)$	$(3,0)$	$(5,2)$	$(4,0)$
$(2,2)$	$(6,2)$	$(1,0)$	$(1,2)$	$(2,0)$
$(5,2)$	$(0,2)$	$(5,0)$	$(2,2)$	$(6,0)$
$(0,0)$	$(3,1)$	$(3,2)$	$(5,1)$	$(4,2)$
$(1,0)$	$(6,1)$	$(1,2)$	$(1,1)$	$(2,2)$
$(2,0)$	$(2,1)$	$(6,2)$	$(4,1)$	$(0,2)$
$(3,0)$	$(5,1)$	$(4,2)$	$(0,1)$	$(5,2)$

Table 4: The table showing $\Delta(D_1, D_2)$

Here, we have highlighted blocks in the table in a similar way to Theorem 3.1. Looking at the $\mathbb{Z}_3$ component, we can observe the same pattern as in Example 3.2 (the corresponding GSEDF in $\mathbb{Z}_7 \times \mathbb{Z}_3$). That is, alternating zeros and ones in the first block, alternating twos and zeros in the second block, and alternating ones and twos in the third block. However, it is clear that the $\mathbb{Z}_7$ components are not following the same pattern. We can see a near pattern as the $\mathbb{Z}_7$ components appear to be the same in all three blocks (aside from the extra row in the third block) but this is broken by the sixth row

$$(5,2)|(0,2)(5,0)(2,0)(6,0)$$

It is interesting to see a similar pattern in the GSEDF table when we know from Example 2.19, that the $(21, 2; 4, 10; 2, 2)$-GSEDF in $\mathbb{Z}_{21} \cong \mathbb{Z}_7 \times \mathbb{Z}_3$ cannot satisfy the conditions for Theorem 2.17.

Whilst the observations made from Table 4 suggest this GSEDF could originate from a recursive construction similar to Theorem 3.1, it does not appear to be the exact same construction. This leaves an interesting area for future research. Perhaps a construction can be found that would ensure the symmetric property required by Theorem 2.17. But even then, there is currently no conversion from direct to semidirect products in this way for any $t > 3$.

4 Difference sets

There is a large amount of literature regarding difference sets. Here, we touch briefly on how difference sets can be used to construct SEDFs and GSEDFs.

Theorem 4.1. [12](Theorem 2.4) Let G be a finite group of size v, and let $A_1, A_2, \ldots, A_m$ be a partition of G, where $|A_i| = k_i \geq 1$. Then $\{A_1, A_2, \ldots, A_m\}$ is a $(v, m; k_1, k_2, \ldots, k_m; \lambda_1, \lambda_2, \ldots, \lambda_m)$-GSEDF in G, if and only if each A_i is a $(v, k_i, k_i - \lambda_i)$-DS in G.

Proof. For any $1 \leq i \leq m$, using multiset operations throughout, we can apply set theory to reach:

$$\begin{aligned}
\bigcup_{1\leq j\leq m: j\neq i} \Delta(A_i, A_j) &= \Delta(A_i, G\backslash A_i) \\
&= \bigcup_{x\in A_i} \Delta(x, G\backslash A_i) \\
&= \bigcup_{x\in A_i} (\Delta(x, G\backslash\{x\})\backslash\Delta(x, A_i\backslash\{x\})) \\
&= (\bigcup_{x\in A_i} \Delta(x, G\backslash\{x\}))\backslash(\bigcup_{x\in A_i} \Delta(x, A_i\backslash\{x\})) \\
&= (\bigcup_{x\in A_i} (G\backslash\{0\}))\backslash\Delta(A_i) \\
&= (k_i(G\backslash\{0\}))\backslash\Delta(A_i).
\end{aligned}$$

And so,

$$\bigcup_{1\leq j\leq m: j\neq i} = \lambda_i(G\backslash\{0\})$$

if and only if

$$\Delta(A_i) = (k_i - \lambda_i)(G\backslash\{0\}).$$

Hence A_i is a $(v, k_i, k_i - \lambda_i)$-DS in G. □

Through the computer search for GSEDFs, it was observed that every GSEDF with $m \geq 3$ was in fact a partition into difference sets. Whilst this was not looked into further within this project, it remains an interesting conjecture to explore.

Corollary 4.2. [15](Corollary 2.2) Let G be a finite group of size v and let $A_1, A_2, \ldots, A_m$ be pairwise disjoint (v, k_i, λ_i') difference sets in G, where $|A_i| = k_i \geq 1$. Let $G\backslash\{A_1, A_2, \ldots, A_m\} = \{g_1, g_2, \ldots, g_r\}$, where $r = v = \sum_{i=1}^{m} k_i$. Then $\{A_1, A_2, \ldots, A_m, \{g_1\}, \{g_2\}, \ldots, \{g_r\}\}$ is a $(v, m+r; k_1, k_2, \ldots, k_m, 1, \ldots, 1; \lambda_1, \lambda_2, \ldots, \lambda_m, 1, \ldots, 1)$-GSEDF in G, where $\lambda_i = k_i - \lambda_i'$ for all $1 \leq i \leq m$.

Proof. For all $1 \leq j \leq r$

$$\begin{aligned}\Delta(g_j) &= \{g_j - g_j\} \\ &= \{0\} = 0(G\backslash\{0\})\end{aligned}$$

So each singleton $\{g_j\}$ is trivially a $(v, 1, 0)$-DS in G. Since

$$(\bigcup_{1\leq i\leq m} A_i) \cup (\bigcup_{1\leq j\leq r} g_j) = G$$

$\{A_1, A_2, \ldots, A_m, \{g_1\}, \{g_2\}, \ldots, \{g_r\}\}$ is a partition of G into (v, k_n, λ_n') difference sets where

$$k_n = \begin{cases} k_i & 1 \leq i \leq m \\ 1 & i \geq m \end{cases}$$

and

$$\lambda_n' = \begin{cases} \lambda_i' & 1 \leq i \leq m \\ 1 & i \geq m \end{cases}$$

So by Theorem 4.1, $\{A_1, A_2, \ldots, A_m, \{g_1\}, \{g_2\}, \ldots, \{g_r\}\}$ is a $(v, m+r; k_1, k_2, \ldots, k_m, 1, \ldots, 1; \lambda_1, \lambda_2, \ldots, \lambda_m, 1, \ldots, 1)$-GSEDF in G, where $\lambda_i = k_i - \lambda_i'$ for all $1 \leq i \leq m$. □

Hence, given just one difference set we can immediately construct a GSEDF. Additionally, we can create many difference GSEDFs from one of the form $\{A_1, A_2, \ldots, A_m, \{g_1\}, \{g_2\}, \ldots, \{g_r\}\}$ by breaking chosen A_i into singletons.

It is interesting to note that the computer search only yielded examples with $m \geq 4$ that were comprised of a difference set padded with its complement in singletons. As above, we focused largely on when m=2 so this remains an open question.

Corollary 4.3. [15](Corollary 2.3) If A is a (v, k, λ)-DS in the finite group G of order v, then $\{A, G\backslash\{A\}\}$ is a $(v, 2; k, n-k; k-\lambda, k-\lambda)$-GSEDF in G.

Proof. The complement of (v, k, λ)-DS is itself a difference set with parameters $(v, v-k, v-2k-\lambda)$ [4](18.4). $A \cup G\backslash A = G$. Hence, this is a partition into difference sets, and so by Theorem 4.1, $\{A, G\backslash\{A\}\}$ is a $(v, 2; k, n-k; k-\lambda, k-\lambda)$-GSEDF in G. □

From Theorem 4.1, it is clear that the existence of a large number of GSEDFs is dependant on the existence of difference sets. However, the latter is a question not yet solved. Whilst, we are able to place restrictions on parameters that allow for certain types of difference sets, we are yet to prove a condition to guarantee the existence of difference sets nor can we classify all difference sets.

5 Cyclotomic Constructions

In this section, we discuss a different method of construction; using cyclotomic numbers. Here, we use the notation $GF(q)$ to represent the unique finite field of order q where q is a prime power. We use $GF(q)^*$ to represent the multiplicative group of order $q-1$ within this field i.e. $GF(q)\backslash\{0\}$. This group is always cyclic, and we call the generator of $GF(q)^*$ the primitive element.

Remark For readability, throughout this section we use the alternative set notation $X + Y$ to represent $X \cup Y$.

5.1 Cyclotomic Numbers

[15] Let θ be the primitive element of $GF(q)^*$, so we can write $GF(q)^* = \langle\theta\rangle$. Additionally, let $e \geq 2$ be a divisor of $q-1$. That is, $q-1 = ef$ for some $f \in \mathbb{Z}$.

Then $C = \langle \theta^e \rangle$ is a cyclic subgroup of $GF(q)$. Furthermore, $|\langle \theta^e \rangle| = f$. The cosets of C in $GF(q)^*$ are the cyclotomic classes of order e in $GF(q)^*$. We denote these cyclotomic classes as

$$C_i^{(e)} = \theta^i C, 0 \leq i \leq e-1.$$

Definition 5.1. [15] The cyclotomic numbers of order e on $GF(q)^*$ (denoted $(i,j)_e$ where $0 \leq i,j \leq e-1$) are defined by

$$(i,j)_e = |(1 + C_i^{(e)}) \cap C_j^{(e)}|.$$

This is equivalent to the number of $x \in C_i^{(e)}$ such that $1 + x \in C_j^{(e)}$.

We will use the following lemma to construct GSEDFs from cyclotomic classes for small values of e.

Lemma 5.2. [6] Let q be a prime power, and $q = ef+1$. For $0 \leq j,l \leq e-1$:

(i) $\Delta(C_j^{(e)}) = \sum_{i=0}^{e-1} (i,0)_e C_{i+j}^{(e)}$

(ii) $\Delta(C_{j+l}^{(e)}, C_l^{(e)}) = \sum_{i=0}^{e-1} (i,j)_e C_{i+l}^{(e)}$

5.2 $e = 2$

Theorem 5.3. If q is prime and $q \equiv 3 \ mod \ 4$ then, $\{\{0\}, C_0^{(2)}, C_1^{(2)}\}$ is a (q,3;1,$\frac{q-1}{2}$, $\frac{q-1}{2}$; 1,$\frac{q+1}{4}$, $\frac{q+1}{4}$)- GSEDF in $GF(q)$

Proof. By definition, $C_0^{(2)} + C_1^{(2)} = GF(q)^*$, and $C_0^{(2)} \cap C_1^{(2)} = \phi$. So $\{\{0\}, C_0^{(2)}, C_1^{(2)}\}$ partitions $GF(q)$.
$\Delta(\{0\}) = 0 \cdot GF(q)^*$, so $\{0\}$ is trivially a $(q,1,0)$-DS. Lemma 5.2 tells us that:
$\Delta(C_j^{(2)}) = \sum_{i=0}^{1} (i,0)_2 C_{i+j}^{(2)}$
$= (0,0)_2 C_j^{(2)} + (1,0)_2 C_{1+j}^{(2)}$
$= \frac{q-3}{4} C_0^{(2)} + \frac{q-3}{4} C_1^{(2)}$
$= \frac{q-3}{4}(C_0^{(2)} + C_1^{(2)})$
$= \frac{q-3}{4} GF(q)^*$
So $C_i^{(2)} (i = 0,1)$ is a (p,$\frac{q-1}{2}$, $\frac{q-3}{4}$)-DS in $GF(p)$. Hence, by Theorem 4.1, $\{\{0\}, \{C_0^{(2)}\}, \{C_1^{(2)}\}\}$ is a $(p,3;1,\frac{n-1}{2},\frac{n-1}{2};1,\frac{p+1}{4},\frac{p+1}{4})$- GSEDF in GF(p). $\square$

5.3 $e = 3$

[5] Let $GF(q)$ be a finite field where q is a prime power such that $q \equiv 1 \pmod 3$. Let $4q = c^2 + 27d^2, c \equiv 1 \; mod \; 3$ where:

- if $p \equiv 2 \; mod \; 3$ then m is even and $d = 0$
- if $p \equiv 1 \; mod \; 3$ then this is the unique proper representation of $4q$ with $c \equiv 1 \; mod \; 3$

For $C_i^{(3)}$ to be a Difference Set in $GF(q)$ we require $\Delta(C_j^{(2)}) = GF(q)^*$.
Equivalently, $(0,0)_e = (1,0)_e = (2,0)_e$.
[5] $(0,0)_e = \frac{1}{9}(q-8+c), (1,0)_e = \frac{1}{18}(2q-4-c-9d), (2,0)_e = \frac{1}{18}(2q-4-c+9d)$.
Hence, $(0,0)_e = (1,0)_e = (2,0)_e = \frac{1}{9}(q-8+c) = \frac{1}{18}(2q-4-c-9d) = \frac{1}{18}(2q-4-c+9d)$ implies $d = 0$ and $c = 4$.
Hence, $4q = 4^2$ so $q = 4$.
When $q = 4$, we have the trivial $(4, 4; 1, 1, 1, 1; 1, 1, 1, 1)$-GSEDF consisting of each element of the group as a singleton. Hence we cannot, in general, construct a GSEDF of the form $\{C_0^{(3)}, C_1^{(3)}, C_2^{(3)}, \{0\}\}$.

5.4 $e = 4$

Theorem 5.4. Let $q = p^m$ be a prime power such that $q = 1 + 4d^2$ where $2 \nmid d$. Then $\{C_0^{(4)}, C_1^{(4)}, C_2^{(4)}, C_3^{(4)}, \{0\}\}$ is a
$(q, 5; \frac{q-1}{4}, \frac{q-1}{4}, \frac{q-1}{4}, \frac{q-1}{4}, 1; \frac{3q+1}{16}, \frac{3q+1}{16}, \frac{3q+1}{16}, \frac{3q+1}{16}, 1)$-GSEDF in $GF(q)$.

We will use the following Theorem from [5] in the proof of Theorem 5.4.

Theorem 5.5. Let $q = p^m \equiv 1 \; mod \; 4$ where p is an odd prime, and write $q = 4f + 1$. Let α be a generator for $GF(q)^*$.
If $p \equiv 3 \; mod \; 4$, let $s = (-p)^{\frac{m}{2}}$ and $t = 0$.
If $p \equiv 1 \; mod \; 4$, define s uniquely by $q = s^2 + t^2, p \nmid s, s \equiv 1 \; mod \; 4$.

Then the cyclotomic numbers of the form $(i, 0)_4$ are defined by the following formulae:

For even f: $(0,0) = \frac{1}{16}(q - 11 - 6s)$

$$(1,0) = (0,1) = (3,3) = \frac{1}{16}(q - 3 + 2s + 4t)$$

$$(2,0) = (0,2) - (2,2) = \frac{1}{16}(q - 3 + 2s)$$

$$(3,0) = (0,3) = (1,1) = \frac{1}{16}(q - 3 + 2s - 4t)$$

$$(1,2) = (1,3) = (2,1) = (2,3) = (3,1) = (3,2) = \frac{1}{16}(q + 1 - 2s)$$

For odd f: $(0,0) = (2,0) = \frac{1}{16}(q - 7 + 2s)$

$$(1,0) = (3,0) = \frac{1}{16}(q - 3 - 2s)$$

Proof of Theorem 5.4. By definition, $C_0^{(4)} + C_1^{(4)} + C_2^{(4)} + C_3^{(4)} = GF(q)^*$, and the $C_i^{(4)}$ are mutually disjoint for all $0 \leq i \leq 3$. Hence,
$\{C_0^{(4)}, C_1^{(4)}, C_2^{(4)}, C_3^{(4)}, \{0\}\}$ partitions $GF(q)$.

From the proof of Theorem 5.3, $\{0\}$ is trivially a $(q, 1, 0)$-DS in $GF(q)$. Lemma 5.2 tells us that:
$\Delta(C_j^{(4)}) = \sum_{i=0}^{3} C_{i+j}^{(4)} = (0,0)C_j^{(4)} + (1,0)C_{1+j}^{(4)} + (2,0)C_{2+j}^{(4)} + (3,0)C_{3+j}^{(4)}$. Now we apply Theorem 5.4. In this case, $f = d^2$ where $2 \nmid d$ so f is odd. We must consider the cases $p \equiv 1 \ mod \ 4$ and $p \equiv 3 \ mod \ 4$.

If $p \equiv 3 \ mod \ 4$, then m must be odd as $p^m = q \equiv 1 \ mod \ 4$. Let $m = 2k$ for some $k \in \mathbb{N}$, then $p^{2k} = (p^k)^2 = 1 + 4d^2$. Since $d \geq 1$,

$$(2d)^2 = 4d^2 < 1 + 4d^2 < 4d^2 + 4d + 1 = (2d + 1)^2.$$

Hence, $(p^k)^2$ lies between two consecutive squares and so cannot be a perfect square itself. This is a contradiction, so $p \not\equiv 3 \ mod \ 4$.

Therefore, $p \equiv 1 \ mod \ 4$, and so we can write $q = 1^2 + (2d)^2$. So $s = 1, t =$

$2d$. Hence,

$$(0,0)C_j^{(4)} + (1,0)C_{1+j}^{(4)} + (2,0)C_{2+j}^{(4)} + (3,0)C_{3+j}^{(4)} =$$
$$\frac{1}{16}(q-7+2)C_j^{(4)} + \frac{1}{16}(q-3-2)C_{1+j}^{(4)} + \frac{1}{16}(q-7+2)C_{2+j}^{(4)} +$$
$$\frac{1}{16}(q-3-2)C_{3+j}^{(4)} =$$
$$\frac{1}{16}(q-5)(C_j^{(4)} + C_{1+j}^{(4)} + C_{2+j}^{(4)} + C_{3+j}^{(4)}) =$$
$$\frac{1}{16}(q-5)(C_0^{(4)} + C_1^{(4)} + C_2^{(4)} + C_3^{(4)}) = \frac{1}{16}(q-5)GF(q)*$$

So $C_j^{(4)}$ is a $(q, \frac{q-1}{4}, \frac{q-5}{16})$-DS in $GF(q)$ for $1 \leq j \leq 3$.
Since, $\frac{q-1}{4} - \frac{q-5}{16} = \frac{4q-4-q+5}{16} = \frac{3q+1}{16}$, by Theorem 4.1,
$\{C_0^{(4)}, C_1^{(4)}, C_2^{(4)}, C_3^{(4)}, \{0\}\}$ is a
$(q, 5; \frac{q-1}{4}, \frac{q-1}{4}, \frac{q-1}{4}, \frac{q-1}{4}, 1; \frac{3q+1}{16}, \frac{3q+1}{16}, \frac{3q+1}{16}, \frac{3q+1}{16}, 1)$-GSEDF in $GF(q)$. □

Remark Theorem 5.4 is stated without proof in [15], however the value of λ_i for $1 \leq i \leq 4$ is given as $\frac{3q-3}{16}$ instead of $\frac{3q+1}{16}$. We believe this to be an error as

$$\frac{3q-3}{16} = \frac{3(1+4d^2)-3}{16} = \frac{12d^2}{16} = \frac{3d^2}{4} \notin \mathbb{Z} \text{ as } 2 \nmid d.$$

5.5 $e = 6$

Here, we omit the proof of several theorems. For detailed proofs of all statements in this section see [14].

The case $e = 6$ does not yield difference sets is the same way we see for $e = 2$ or $e = 4$.

Theorem 5.6. [14](Part 1, Theorem 16) If $q = 6f + 1$, then $C_0^{(6)}$ is not a difference set in $GF(q)$. Additionally, $C_0^{(6)} + \{0\}$ is not a difference set in $GF(q)$.

However, whilst we cannot simply partition $GF(q)$ into its cyclotomic classes and the identity to form a GSEDF, we can construct a difference set by combining certain classes together.

Theorem 5.7. [14](Part 1, Theorem 18) If $q = 27 + d^2 = 6f + 1$, then $C_0^{(6)} + C_1^{(6)} + C_3^{(6)}$ is a difference set in $GF(q)$.

Since the complement of a difference set is itself a difference set [4](18.4), $C_2^{(6)} + C_4^{(6)} + C_5^{(6)} + \{0\}$ is a difference set in $GF(q)$. Therefore,

$$\{\{C_0^{(6)}, C_1^{(6)}, C_3^{(6)}\}, \{C_2^{(6)}, C_4^{(6)}, C_5^{(6)}\{0\}\}\}$$

is a GSEDF in $GF(q)$.

6 Further work

We aimed to provide a comprehensive overview of known constructions of GSEDFs, with a particular focus on groups of order less than 50. Whilst, many constructions have already been put forward, there is often a large focus on abelian groups, so there are several examples of GSEDFs within non abelian finite groups that remain unexplained. The extension of Theorem 2.9 to semidirect products $\mathbb{Z}_n \rtimes \mathbb{Z}_i$ for $i > 2$ is a particularly interesting area for further research.

Paying extra attention to group structure could provide some clarity as to why some parameters exist across different groups with the same order, and others can only exist in one. For example, what GSEDFs exist in the cyclic group $\mathbb{Z}_n$ but not in a direct or semidirect product of the same order? A similar question to this would be considering two non-equivalent GSEDFs with the same parameters within the same group. Several examples of this occurring were found.

In addition, the conditions that cause difference sets to arise persist as a mystery. We know it is only for certain orders of group that difference sets can be found, however most texts can only go as far as to provide examples rather than a concrete pattern. Being able to confidently state whether a partition into difference set is possible would unlock many more GSEDFs, especially when group order becomes higher than reasonable examples.

Furthermore, much of the literature and this report focuses on the case when $m = 2$. In fact, all GSEDFs with $m > 2$ discussed here or found in our computer search arise from a partition into difference sets. Is this the only possibility or can we extend constructions with $m = 2$, such as the recursive construction in Theorem 3.1, for $m \geq 3$?

7 Acknowledgments

I would like to thank my supervisor Dr Sophie Huczynska for all her guidance and support throughout this project. Her time and knowledge have been invaluable, and I could not have wished for a better experience.

Additionally, I am grateful to Lord Laidlaw and the Laidlaw Foundation for their generous funding through the Laidlaw Research and Leadership Programme. A special thanks to the St Andrews Laidlaw team for their continued support throughout this process.

References

[1] Ahmed Ayache and Khalid Amin. *Introduction to Group Theory*. en. University Texts in the Mathematical Sciences. Singapore: Springer Nature, 2025. ISBN: 9789819766468. DOI: 10.1007/978-981-97-6647-5. URL: https://link.springer.com/10.1007/978-981-97-6647-5.

[2] Wayne D. Blizard. "Multiset Theory". In: *Notre Dame Journal of Formal Logic* 30.1 (1989), pp. 36–66. DOI: 10.1305/ndjfl/1093634995.

[3] D. de Caen et al. "Near-factors of finite groups". In: *Ars Combin.* 29 (1990), pp. 53–63. ISSN: 0381-7032,2817-5204.

[4] Charles J. Colbourn and Jeffrey H. Dinitz. *Handbook of combinatorial designs edited by Charles J. Colbourn, Jeffrey H. Dinitz*. Chapman & Hall/Taylor & Francis, 2007.

[5] Sophie Huczynska and Laura M. Johnson. "Internal and external partial difference families and cyclotomy". In: *Discrete Math.* 346.3 (2023), Paper No. 113295, 24. ISSN: 0012-365X,1872-681X. DOI: 10.1016/j.disc.2022.113295. URL: https://doi.org/10.1016/j.disc.2022.113295.

[6] Sophie Huczynska and Tekgül Kalaycı. *Cyclotomic skew partial difference sets and partial difference families*. 2026. arXiv: 2605.19596 [math.CO]. URL: https://arxiv.org/abs/2605.19596.

[7] Donald L. Kreher, Shuxing Li, and Douglas R. Stinson. "λ-fold near-factorizations of groups". In: *Des. Codes Cryptogr.* 94.5 (2026), Paper No. 106, 34. ISSN: 0925-1022,1573-7586. DOI: 10.1007/s10623-026-01825-x. URL: https://doi.org/10.1007/s10623-026-01825-x.

[8] Donald L. Kreher, William J. Martin, and Douglas R. Stinson. "Uniqueness and explicit computation of mates in near-factorizations". In: *J. Algebraic Combin.* 63.4 (2026), Paper No. 53, 21. ISSN: 0925-9899,1572-9192. DOI: 10.1007/s10801-026-01542-7. URL: https://doi.org/10.1007/s10801-026-01542-7.

[9] Donald L. Kreher, Maura B. Paterson, and Douglas R. Stinson. "Near-factorizations of dihedral groups". In: *Des. Codes Cryptogr.* 93.11 (2025), pp. 5015–5038. ISSN: 0925-1022,1573-7586. DOI: 10.1007/s10623-025-01715-8. URL: https://doi.org/10.1007/s10623-025-01715-8.

[10] Xiaojuan Lu, Xiaolei Niu, and Haitao Cao. "Some results on generalized strong external difference families". In: *Des. Codes Cryptogr.* 86.12 (2018), pp. 2857–2868. ISSN: 0925-1022,1573-7586. DOI: 10.1007/s10623-018-0481-6. URL: https://doi.org/10.1007/s10623-018-0481-6.

[11] Wakaha Ogata et al. "New combinatorial designs and their applications to authentication codes and secret sharing schemes". In: vol. 279. 1-3. In honour of Zhu Lie. 2004, pp. 383–405. DOI: 10.1016/S0012-365X(03)00283-8. URL: https://doi.org/10.1016/S0012-365X(03)00283-8.

[12] Maura B. Paterson and Douglas R. Stinson. "Combinatorial characterizations of algebraic manipulation detection codes involving generalized difference families". In: *Discrete Math.* 339.12 (2016), pp. 2891–2906. ISSN: 0012-365X,1872-681X. DOI: 10.1016/j.disc.2016.06.004. URL: https://doi.org/10.1016/j.disc.2016.06.004.

[13] Arnaud Pêcher. "Cayley partitionable graphs and near-factorizations of finite groups". In: vol. 276. 1-3. 6th International Conference on Graph Theory. 2004, pp. 295–311. DOI: 10.1016/S0012-365X(03)00293-0. URL: https://doi.org/10.1016/S0012-365X(03)00293-0.

[14] T. Storer. *Cyclotomy and difference sets*. Lectures in Advanced Mathematics 2. Chicago, Ill.: Markham Publishing Co., 1967. vii+134.

[15] Jiejing Wen et al. "Cyclotomic construction of strong external difference families in finite fields". In: *Des. Codes Cryptogr.* 86.5 (2018), pp. 1149–1159. ISSN: 0925-1022,1573-7586. DOI: 10.1007/s10623-017-0384-y. URL: https://doi.org/10.1007/s10623-017-0384-y.